Муниципальное бюджетное дошкольное образовательное учреждение

«Центр развития ребёнка – детский сад №50 «Непоседа»

|  |  |
| --- | --- |
| СОГЛАСОВАНОПредседателем профкомаПротокол № 13 от «20» октября 2021г. | УТВЕРЖДЕНОприказом заведующего МБДОУ «Центр развития ребенка – детский сад № 50 «Непоседа»Приказ № 336 от «20» октября 2021 г. |

|  |
| --- |
|  |
| **ПОЛИТИКА****ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ****ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ** |
| г. Новочебоксарск 2021 |

Содержание

[Определения 1](#_TOC_250021)

[Введение 8](#_TOC_250020)

1. [Общие положения 9](#_TOC_250019)
2. [Область действия 10](#_TOC_250018)
3. [Система защиты персональных данных 12](#_TOC_250017)
4. [Требования к подсистемам СЗПДн 14](#_TOC_250016)
	1. [Подсистемы управления доступом, регистрации и учета 14](#_TOC_250015)
	2. [Подсистема обеспечения целостности и доступности 15](#_TOC_250014)
	3. [Подсистема антивирусной защиты 15](#_TOC_250013)
	4. [Подсистема анализа защищенности 15](#_TOC_250011)
	5. [Подсистема обнаружения вторжений 16](#_TOC_250010)
5. [Пользователи ИСПДн 17](#_TOC_250008)
	1. [Администратор ИСПДн 17](#_TOC_250007)
	2. Администратор безопасности 17
	3. [Оператор АРМ 18](#_TOC_250006)
6. [Требования к персоналу по обеспечению защиты ПДн 19](#_TOC_250002)
7. [Должностные обязанности пользователей ИСПДн 21](#_TOC_250001)
8. Список использованных источников 22

# Определения

В настоящем документе используются следующие термины и их определения.

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** – подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Биометрические персональные данные** – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность и которые используются Администрацией для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных (включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию).

**Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими

средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** – возможность получения информации и ее использования.

**Закладочное устройство** – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

**Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

**Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Использование персональных данных** – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

**Межсетевой экран** – локальное (однокомпонентное) или функционально- распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Неавтоматизированная обработка персональных данных** – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

**Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

**Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде

символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обезличивание персональных данных** – действия, в результате которых становится невозможно без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

**Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

**Общедоступные персональные данные** – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

**Оператор (персональных данных)** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

**Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно- цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

**Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Политика «чистого стола»** – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

**Пользователь информационной системы персональных данных** – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

**Программное (программно-математическое) воздействие** – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Раскрытие персональных данных** – умышленное или случайное нарушение конфиденциальности персональных данных.

**Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Специальные категории персональных данных** – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Трансграничная передача персональных данных** – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость** – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

|  |  |
| --- | --- |
| АВС | – антивирусные средства |
| АРМ | – автоматизированное рабочее место |
| ВТСС |  – вспомогательные технические средства и системы |
| ИСПДн | – информационная система персональных данных |
| КЗ | – контролируемая зона |
| ЛВС | – локальная вычислительная сеть |
| МЭ | – межсетевой экран |
| НСД | – несанкционированный доступ |
| ОС | – операционная система |
| ПДн | – персональные данные |
| ПМВ | – программно-математическое воздействие |
| ПО | – программное обеспечение |
| ПЭМИН | – побочные электромагнитные излучения и наводки |
| САЗ | – система анализа защищенности |
| СЗИ | – средства защиты информации |
| СЗПДн | – система (подсистема) защиты персональных данных |
| СОВ | – система обнаружения вторжений |
| ТКУИ |  – технические каналы утечки информации |
| УБПДн | – угрозы безопасности персональных данных |

# ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее Политика) МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» является официальным документом.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 1 ноября 2012 года

№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании:

* «Типовых требований по организации и обеспечению функционирова- ния шифровальных (криптографических) средств, предназначенных для за- щиты информации, не содержащей сведений, составляющих государствен- ную тайну в случае из использования для обеспечения безопасности персо- нальных данных при их обработке в информационных системах персональ- ных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа».

# Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения персональных данных.

Состав объектов защиты представлен в Перечне персональных данных, указанному в Положении об обработке персональных данных.

Состав ИСПДн, подлежащих защите, представлен в Акте определения уровня защищенности персональных данных в ИСПДн.

# Область действия

Требования настоящей Политики распространяются на всех сотрудников МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

# Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

* Акта определения уровня защищенности персональных данных в ИСПДн;
* Перечня персональных данных, подлежащих защите;
* Частных моделей актуальных угроз и вероятного нарушителя ИСПДн;
* Положения о разграничении прав доступа к персональным данным;
* Руководящих документов ФСТЭК и ФСБ России.

Для обеспечения защиты ИСПДн необходимо соблюдение организационно-технических мер. Администрацией обеспечивается безопасность персональных данных в соответствии с необходимым уровнем защищенности, которая описана в Техническом задании на создание системы защиты для ИСПДн. В МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» определены актуальные угрозы безопасности ПДн, которые описаны в Модели актуальных угроз и вероятного нарушителя ИСПДн.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных

(недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа». На основании анализа актуальных угроз безопасности ПДн, описанного в Частной модели актуальных угроз и вероятного нарушителя ИСПДн делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по защите персональных данных.

Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а также программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

* АРМ пользователей;
* Сервера приложений;
* СУБД;
* Граница ЛВС;
* Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищённости ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

* антивирусные средства для рабочих станций пользователей и серве-

ров;

* средства межсетевого экранирования;
* средства криптографической защиты информации, при передаче за-

щищаемой информации по каналам связи.

Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

* + управление и разграничение доступа пользователей;
	+ регистрацию и учёт действий с информацией;
* обеспечивать целостность данных;
* производить обнаружений вторжений.

Список используемых технических средств отражается в Плане мероприятий по защите персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены заведующим МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» или лицом, ответственным за обеспечение защиты ПДн.

# Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

* управления доступом, регистрации и учета;
* обеспечения целостности и доступности;
* антивирусной защиты;
* анализа защищенности;
* обнаружения вторжений;

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн.

# Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учёта предназначена для реализации следующих функций:

* идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
* идентификации терминалов, узлов сети, каналов связи, внешних уст- ройств по логическим именам;
* идентификации программ, томов, каталогов, файлов, записей, полей за- писей по именам;
* регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее ос- танова.
* регистрации попыток доступа программных средств (программ, процес- сов, задач, заданий) к защищаемым файлам;
* регистрации попыток доступа программных средств к терминалам, кана- лам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и

СУБД). Также может быть внедрено специальное техническое средство или их комплекс, осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учётных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

# Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа», а также средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

# Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа». Средства антивирусной защиты предназначены для реализации следующих функций:

* резидентный антивирусный мониторинг;
* антивирусное сканирование;
* скрипт-блокирование;
* централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчётов и статистиче- ской информации по работе продукта;
* автоматизированное обновление антивирусных баз;
* ограничение прав пользователя на остановку исполняемых задач и из- менения настроек антивирусного программного обеспечения;
* автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путём внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

# Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

# Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн, подключённые к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

# Пользователи ИСПДн

В ИСПДн МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

* Администратор ИСПДн;
* Администратора безопасности ИСПДн;
* Оператор АРМ;

Данные о группах пользователях, уровне их доступа и информированности должен быть отражён в Положении о разграничении прав доступа к персональным данным.

# Администратор ИСПДн

Администратор ИСПДн, сотрудник МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа», ответственный за настройку, внедрение и сопровождение ИСПДн, обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

* обладает полной информацией о системном и прикладном программ- ном обеспечении ИСПДн;
* обладает полной информацией о технических средствах и конфигурации ИСПДн;
* имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
* обладает правами конфигурирования и административной настройки технических средств ИСПДн.

# Администратор безопасности ИСПДн

 Администратор безопасности ИСПДн, сотрудник МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа», ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонентов.

Администратор безопасности ИСПДн обладает следующим уровнем доступа и знаний:

* обладает правами Администратора ИСПДн;
* обладает полной информацией об ИСПДн;
* имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
* не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности ИСПДн уполномочен:

* реализовывать политику безопасности в части настройки СКЗИ и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
* осуществлять аудит средств защиты;
* устанавливать доверительные отношения своей защищенной сети с се- тями других организаций.

# Оператор АРМ

Оператор АРМ, сотрудник МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа», осуществляющий обработку ПДн. Обработка ПДн включает:

* возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн,
* формирование справок и отчётов по информации, полученной из ИСПДн.

Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

* обладает всеми необходимыми атрибутами (например, паролем), обес- печивающими доступ к некоторому подмножеству ПДн;
* располагает конфиденциальными данными, к которым имеет доступ.

# Требования к персоналу по обеспечению защиты ПДн

Все сотрудники МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа», являющиеся пользователями ИСПДн, должны чётко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа». При работе с ПДн в ИСПДн сотрудники МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утверждённой формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили Политику информационной безопасности и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

# Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

* Инструкция администратора ИСПДн;
* Инструкция администратора безопасности ИСПДн;
* Инструкция пользователя ИСПДн.

Ответственность сотрудников ИСПДн МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа».

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администратор ИСПДн и администратор безопасности ИСПДн несут ответственность за все действия, совершённые от имени их учётных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа» – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников МБДОУ «Центр развития ребенка – детский сад №50 «Непоседа».

# Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение являются:

1. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных дан- ных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
2. Постановление Правительства Российской Федерации от 1ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
3. «Положение об особенностях обработки персональных данных, осуще- ствляемой без использования средств автоматизации», утверждённое Поста- новлением Правительства РФ от 15.09.2008 г. № 687.
4. «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утверждённые Постановлением Правительства РФ от 06.07.2008 г. № 512.
5. Нормативно-методические документы Федеральной службы по техниче скому и экспертному контролю Российской Федерации (далее - ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн.
6. Базовая модель угроз безопасности персональных данных при их обра- ботке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г.
7. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г

**Лист ознакомления с Политикой информационной безопасности**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **ФИО** | **Должность** | **Дата** | **Подпись** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |
| 9 |  |  |  |  |
| 10 |  |  |  |  |
| 11 |  |  |  |  |
| 12 |  |  |  |  |
| 13 |  |  |  |  |
| 14 |  |  |  |  |
| 15 |  |  |  |  |
| 16 |  |  |  |  |
| 17 |  |  |  |  |
| 18 |  |  |  |  |
| 19 |  |  |  |  |
| 20 |  |  |  |  |
| 21 |  |  |  |  |
| 22 |  |  |  |  |
| 23 |  |  |  |  |
| 24 |  |  |  |  |
| 25 |  |  |  |  |
| 26 |  |  |  |  |
| 27 |  |  |  |  |
| 28 |  |  |  |  |
| 29 |  |  |  |  |
| 30 |  |  |  |  |
| 31 |  |  |  |  |
| 32 |  |  |  |  |
| 33 |  |  |  |  |
| 34 |  |  |  |  |
| 35 |  |  |  |  |
| 36 |  |  |  |  |
| 37 |  |  |  |  |
| 38 |  |  |  |  |
| 39 |  |  |  |  |
| 40 |  |  |  |  |